Don Springmeyer, Esq. (NBN 1021)
KEMP JONES, LLP
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, NV 89169
Tel: (702) 385-6000
Email: d.springmeyer@kempjones.com

Counsel for Plaintiff

(Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

DAVID LACKEY, *individually and on behalf of all other similarly situated,* Plaintiff, v. **CAESARS ENTERTAINMENT, INC.,** Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff David Lackey ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Caesars Entertainment, Inc. ("Defendant" or "Caesars") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

I. INTRODUCTION

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a cyberattack on Caesars on or around September 7, 2023 (the "Data Breach"). Caesars has not disclosed the exact number of individuals impacted by the Data Breach, but it has confirmed that the cybercriminals were able to obtain a copy of Caesar's loyalty program database, including the driver's license numbers and Social Security numbers for a "significant number" of its more than 65 million program members.[1] The Data Breach was directly caused by the Defendant's failure to properly protect and secure the personally identifiable information ("PII") of its customers—in particular, members of its loyalty program.

2. Reportedly, the cyber-attack that led to the Data Breach was conducted by a cybercriminal organization known as Scattered Spider, thought to be mostly made up of individuals in their late teens and early 20s, that specializes in gaining access credentials to a target's data systems by impersonating people in the organization through convincing phone calls.[2] The Data Breach reportedly originated from a social engineering attack on the company's outside IT vendor, which allowed the hackers access to the loyalty program database.[3]

---

[1] https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/ (last accessed Sept. 27, 2023); https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins (last accessed Sept, 27, 2023).

[2] https://www.vox.com/technology/2023/9/15/23875113/Caesars-hack-casino-vishing-cybersecurity-ransomware (last accessed Sept. 26, 2023).

[3] https://www.stltoday.com/news/local/business/casino-giant-caesars-entertainment-confirms-data-breach/article_899b3b88-530b-11ee-9ed2-6b827d6c3b22.html (last accessed Sept. 27, 2023).

3. According to Caesars, it has one of the largest loyalty programs in the gaming industry, with over 65 million members.[4] Caesars has the "largest and most diverse collection of gaming destinations in the U.S." and considers itself as a "global leader in gaming and hospitality".[5] Based on available information, and belief, the Caesars' Data Breach likely involves millions of its customers' PII.

4. Caesars' Rewards program allows members to earn credits that they can use on a variety of services offered by Caesars, including gambling, hotel reservations, dining, and shopping.[6] However, to participate in the program, members must consent to the "collection and use of Member personal information" in accordance with Caesars' privacy policy.[7]

5. In its privacy policy, Caesars informs its Rewards program members that it may collect a large range of PII including first and last name, address, phone number, email address, credit card number, Social Security number, driver license number, passport number, license plate number, geolocation information, Caesars Rewards number, date of birth, purchase information, gaming activity information, biometric information, health information, and other similar information.[8]

6. After gaining access to Caesars' systems, the hackers extracted the loyalty member database and demanded Caesar's pay a $30 million ransom.[9] According to reports, Caesars agreed to pay roughly half of the ransom demand to the hackers.[10]

7. Individuals, including Plaintiff and Class Members, were customers of Defendant's gaming and entertainment services and/or members of Defendant's Rewards program. Defendant

[4] https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins (last accessed Sept. 27, 2023).

[5] https://newsroom.caesars.com/overview/default.aspx (last accessed Sept. 28, 2023).

[6] https://www.caesars.com/myrewards/earn-and-redeem (last visited Sept. 27, 2023).

[7] https://www.caesars.com/myrewards/caesars-rewards-rules-regs (last visited Sept. 27, 2023).

[8] https://www.caesars.com/corporate/privacy (last accessed Sept. 27, 2023).

[9] Id.

[10] Id.

requires individuals, including Plaintiff and Class Members, to provide highly sensitive PII as a prerequisite to use Defendant's entertainment services and to join Caesars' Rewards loyalty program. As an incentive to provide this information, Defendant's loyalty program allows its members to obtain points that may be exchanged for program rewards. By obtaining, using, and deriving a benefit from Plaintiff's and Class Member' PII, Caesars assumed legal and equitable duties to Plaintiff and Class Members to safeguard that information and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. Plaintiff and Class Members had a reasonable expectation and understanding that Defendant would adopt reasonable data security safeguards to protect PII. Defendant failed to do so, leading to the Data Breach.

8. Caesars owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their PII. Yet, Caesars maintained this PII in a negligent and/or reckless manner and maintained the PII in a condition which left it vulnerable to cyberattacks.

9. The Data Breach was a direct result of Caesars' failure to implement reasonable data security measures to protect Class Members' PII against unauthorized intrusions and access.

10. As a result of the Data Breach, Plaintiff, and Class Members, have been damaged in several ways. Plaintiff and Class Members have been exposed to an increased risk of fraud, identity theft, and other misuse of their PII. Plaintiff and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. To protect themselves from this increased risk of fraud, Plaintiff and Class Members may be forced to purchase credit monitoring and other identity protection services, purchase credit reports, place credit freezes and fraud alerts on their credit reports and spend time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class Members have also suffered "benefit of the bargain" damages because they paid money to Caesars for services that were intended to be accompanied by adequate data security but were not. Plaintiff and Class Members also suffered a "loss of value of PII" resulting from the Data Breach.

11. PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources (such as publicly available information, social media, etc.) to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails and text messages to Class Members to trick them into revealing sensitive information such as Social Security numbers, financial account numbers, login credentials, and the like. Thieves can also send emails and text messages embedded with ransomware.

12. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated consumers whose PII was stolen in the Data Breach. Plaintiff seeks remedies including: (i) compensation for the theft and misuse of their data; (ii) reimbursement of out-of-pocket costs; (iii) compensation for time spent responding to the Data Breach; (iv) comprehensive identify protection services paid for by Caesars; (v) injunctive relief requiring substantial improvements to Caesars' data security practices, as detailed below.

II. PARTIES

A. Plaintiff

13. Plaintiff David Lackey is a natural person, resident, and citizen of the State of Virginia.

14. Defendant Caesars obtained and continues to maintain the PII of Plaintiff via his participation in the Caesars' Rewards loyalty program. Defendant owed Plaintiff a legal duty and obligation to protect his PII from unauthorized access and disclosure. Plaintiff's PII was compromised and disclosed as a result of Defendant's inadequate data security practices, which resulted in the Data Breach.

15. Plaintiff has been a member of the Caesars' Rewards program for over twenty years. He has attended and used his Caesars' Rewards membership at Caesars' in Las Vegas, Nevada, and in the past year, has stayed a Caesars property on four separate occasions.

B. Defendant

16. Defendant Caesars Entertainment, Inc. is a publicly traded company incorporated

in Delaware with its principal place of business at 100 West Liberty Street, 12th Floor, Reno, NV 89501. It is a global hospitality and gaming company that owns, operates, and manages hotels, casinos, and resorts located predominantly in Nevada. Caesars' portfolio of Las Vegas properties includes Caesars' Place Las Vegas, The Cromwell, Flamingo Las Vegas, Horseshoe Las Vegas, The LINQ Hotel & Casino, Paris Las Vegas, Planet Hollywood Resort & Casino, Harrah's Las Vegas, and Rio All-Suite and Casino.[11] Caesars' net revenue in 2022 was approximately $10 billion and net income was approximately $1 billion.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over the action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than 100 Class Members, and Plaintiff and at least one Class member is a citizen of a state different than Defendant.

18. This Court has diversity jurisdiction over Plaintiff's claims pursuant to 29 U.S.C. § 1332(a)(1) because Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds $75,000.

19. This Court has general personal jurisdiction over Caesars because Caesars maintains its principal place of business in this District. This Court also has specific personal jurisdiction over Caesars because Caesars engaged in the conduct underlying this action in this District, including the collection, storage, and inadequate safeguarding of Plaintiff's PII.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Caesars is based in this District, entered into consumer transactions with Plaintiff in this District, and made its data security decisions leading to the Data Breach in this District.

[11] *See* Caesars Entertainment, Inc. Form 10-K for the year ended Dec. 31, 2022, at pg. 28 *available at* https://investor.caesars.com/static-files/abff6ce9-34b1-4057-9c78-db6bf146c295 (last visited Sept. 28, 2023).

IV. STATEMENT OF FACTS

A. The Caesars Data Breach

21. On or about September 7, 2023, the Defendant filed a Form 8-K with the SEC in which Caesars disclosed that it had been the target of a cyberattack that led to a data breach.[12] The report stated:

> Caesars Entertainment, Inc. (the "Company," "we," or "our") recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. Our customer-facing operations, including our physical properties and our online and mobile gaming applications, have not been impacted by this incident and continue without disruption.
>
> After detecting the suspicious activity, we quickly activated our incident response protocols and implemented a series of containment and remediation measures to reinforce the security of our information technology network. We also launched an investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. As a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, among other data, our loyalty program database, which includes driver's license numbers and/or social security numbers for a significant number of members in the database. We are still investigating the extent of any additional personal or otherwise sensitive information contained in the files acquired by the unauthorized actor. We have no evidence to date that any member passwords/PINs, bank account information, or payment card information (PCI) were acquired by the unauthorized actor.

22. Around the same time as the filing of the 8-K, Caesars released a similar statement on its Informational Website informing the public that a social engineering attack on one of its outsourced IT support vendors had led to an unauthorized actor acquiring Caesars' loyalty program database—including the driver's license numbers and/or Social Security numbers of a significant number of its members.[13]

23. Both the 8-K and Caesars' statement on its website leave crucial questions

[12] *See* SEC Form 8-K, Caesars Entertainment, Inc., Sept. 7, 2023, available at https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57 (last accessed Sept. 28, 2023).

[13] *See* Caesars Informational Website, Learn More, https://response.idx.us/caesars/#learn-more (last accessed Sept. 28, 2023).

unanswered. Caesars has not, to this date, disclosed: how many of its loyalty rewards program members were affected by the Data Breach; what information was taken; how the cybercriminals were able to exploit vulnerabilities in Caesars' data systems; the identity of Caesars' outside IT vendor; the identity of the hacking group responsible for the Data Breach; or what steps Caesars has taken to ensure that such an attack does not happen again.

24. Even though Caesars has not disclosed the identity of the hackers, reports indicate that Scattered Spider, a group that specializes in social engineering attacks, was responsible for the Data Breach.[14] The same group is allegedly responsible for a similar cyberattack of Caesars' competitor, MGM Resorts International, that occurred around the same time and that also resulted in a data breach.[15] Caesars has reportedly paid the hackers approximately $15 million in ransom to ensure that the data is not disclosed.[16]

25. Although Caesars has not disclosed precisely the nature of the data obtained in the Data Breach, upon information and belief, the data likely consists of PII including names, addresses, phone numbers, email addresses, and dates of birth, as well as driver's license numbers, and Social Security numbers.[17] Cyber security journalists have characterized PII stolen in a previous data breach as a "treasure trove" of "highly sensitive" personal information, and that affected consumers now face a risk of misuse of their PII.[18] Yet, at this time, Caesars has still not disclosed the number of individuals impacted by the Data Breach, or precisely what forms of PII

[14] https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/ (last accessed Sept. 28, 2023).

[15] Id.

[16] Id.

[17] https://www.reuters.com/business/casino-giant-Caesars-confirms-data-breach-2023-09-14/ (last accessed Sept. 26, 2023).

[18] *See Details of 10.6 Million CAESARS Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19, 2020, *available at* https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-Caesars-hotel-guests-posted-on-a-hacking-forum/ (last visited Sept. 26, 2023); *accord CAESARS Resorts Hack Exposes Details of 10.6 Million Guests*, Fortune, Feb. 20, 2020, *available at* https://fortune.com/2020/02/20/Caesars-resorts-hack-data-breach-10-6-million-guests/ ("Identity theft is the big threat here.") (last visited Sept. 26, 2023).

were taken.

26. As a multi-billion-dollar publicly traded company, Caesars had the financial wherewithal and personnel necessary to prevent the Data Breach. Yet, Caesars nevertheless failed to adopt adequate data security measures.

27. As a condition of joining Caesars' loyalty program, Caesars requires that its customers entrust it with highly sensitive PII. Caesars retains and stores this information to use for marketing purposes, to develop new products and services, to do statistical analysis, and many other things.[19] By obtaining, collecting, and deriving a benefit from its customers' PII, Caesars assumed legal and equitable duties to take reasonable measures to protect their PII. Caesars failed to do so, despite the known risk of theft by cyber criminals.

B. Criminals Will Continue to Use the Stolen PII for Years

28. The risk of fraud following a data breach like this one persists for years. Identity thieves often hold stolen data for months or years before using it, to avoid detection and maximize profits. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because data is often broken into smaller batches when sold or re-sold to appeal to different types of buyers. In addition, stolen data may be distributed through off-line criminal networks and syndicated to be used for crime near where the victim resides.

29. According to a Government Accountability Office Report, the threat of future identity theft lingers for a substantial period of time after a data breach given the time lag between when information is stolen and when it is used:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure

[19] https://www.caesars.com/corporate/privacy

the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

30. Another source, discussing a previous data breach of Caesars' competitor MGM Resorts International, stated: "[A]s with many breaches, malicious actors sometimes wait months or years to tip their hand. . . . This is a great example of how these breaches and their fallout can continue to haunt businesses for quite some time. . . . "[21]

31. Accordingly, Class Members may not see the full extent of identity theft or misuse of their personal information for years to come. They face an ongoing risk and must vigilantly monitor their financial and other accounts indefinitely.

32. Moreover, even after Class Members' PII is misused, it may take months or years for them to become aware of the misuse. This complicates the process of disputing and correcting the misuse of their data.

C. PII Stolen in the Data Breach Can be Combined with Data Acquired Elsewhere to Commit Identity Theft

33. Identity thieves can combine PII stolen in the Data Breach with information gathered from other sources such as public sources or even the consumer's social media accounts, to commit identity theft. Thieves can then use the combined data profile to commit fraud including, among other things, opening new financial accounts or taking out loans in the consumer's name, using the consumer's information to obtain government benefits, filing fraudulent tax returns using the consumer's information and retaining the resulting tax refunds, obtaining a driver's licenses in the consumer's name but with another person's photograph, and giving false information to police during an arrest.

---

[20] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 26, 2023).

[21] *See MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, *available at* https://www.scmagazine.com/news/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers (last visited Sept. 26, 2023).

34. A federal district court has explained the process as follows:

> The threat of identity theft is exacerbated by what hackers refer to as "fullz packages." A fullz package is a dossier that compiles information about a victim from a variety of legal and illegal sources. Hackers can take information obtained in one data breach and cross-reference it against information obtained in other hacks and data breaches. So, for example, if a hacker obtains a victim's . . . health information from UnityPoint, the hacker can combine it with the same victim's Social Security number and phone number from a different data breach. This allows the hacker to compile a full record of information about the individual, which the hacker then sells to others as a package.

Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 789 (W.D. Wis. 2019).

35. Thieves can also use PII from the Data Breach, alone or in combination with other information about the consumer, to send highly targeted spear-phishing emails to the consumer to obtain more sensitive information. Spear phishing involves sending emails that look legitimate and are accompanied by correct personal and other information about the individual. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Bank of America, Amazon, or even a government entity), the individual provides sensitive information requested in the email. This could include login credentials, account numbers, or various other types of information.

36. Identity thieves can also use PII from the Data Breach in a "SIM swapping" attack to take control of consumers' phone numbers, allowing them to bypass 2-factor authentication to access the consumer's most sensitive accounts. In other words, fraudsters can use breached PII to convince the consumer's mobile phone carrier to port-over the person's mobile phone number to a phone that the hacker controls. A journalist discussing a previous Data Breach of Caesars' competitor MGM described this scheme as follows:

> Exposed phone numbers create an additional risk: SIM swapping. In these scams, criminals use the data they've gathered about a potential victim to convince wireless carriers to move a number to a different phone. The goal is

to intercept two-factor authentication codes that are delivered by SMS.[22]

D. Caesars Uses Consumers' PII for Profit-Generating Purposes

37. Consumers' PII is also valuable to Caesars. Caesars recognizes a business value of PII and collects it to better target customers and increase its profits.

38. Caesars acknowledges in its privacy policy that it uses consumers' PII for the following purposes:

- to operate our Caesars Rewards program and provide information to you about your Caesars Rewards program activity;
- to improve the products and services we provide you and develop new products and services;
- to improve our properties, websites and mobile apps;
- to track your use of our properties, websites and mobile apps for our internal market research and analytics;
- to create a more accurate and complete customer profile for you to better understand and predict the products and services you want to use and to provide a more personalized level of service;
- to notify you about promotions and special offers regarding products and services provided by us or our affiliates or other associated third parties, including our business partners;
- to ask for your participation in our internal market research;
- to generate aggregate statistical studies about our customers to better understand how our customers use our services;
- to contact you in response to your inquiries, comments and suggestions;
- to provide a healthy, secure, and safe environment for our customers or employees;
- to protect and defend our rights or property or enforce our agreements with you;
- to perform background checks for any reason (to the extent permitted by applicable laws), which includes but is not limited to any investigation into your identity, any credit checks or any inquiries into your personal history:
- to cash your checks, extend you credit, process credit card, ACH and/or other financial transactions;
- administer general recordkeeping for financial statements and audits;

[22] *See For Sale: Hacked Data On 142 Million MGM Hotel Guests*, Forbes, July 14, 2020, *available at* https://www.forbes.com/sites/leemathews/2020/07/14/mgm-142-million-guests-hacked/?sh=1ca9d7125294 (last visited Sept. 26, 2023).

- comply with our internal records management policy and retention rules;
- to contact you otherwise when necessary; and
- otherwise with your consent or as permitted or required by law.[23]

39. It also acknowledges in privacy policy that it shares its customers PII to third parties.[24]

40. Caesars' self-serving motive to retain and mine its customers' PII led to Caesars holding a trove of customer data. Caesars was unjustly enriched by retaining consumers' PII for its own profit motive, while failing to adopt reasonable data security measures to protect that PII.

E. Plaintiff and Class Members Suffered Damages

41. Caesars' failure to keep the PII of Plaintiff and Class Members secure has severe ramifications. Plaintiff and Class Members face a high risk of misuse of their PII from the Data Breach. Upon information and belief, the hackers stole PII from Caesars with the specific intent to use it for illicit purposes and/or sell it to others to be misused. And the hackers have carried out this intent by using the data to demand a ransom payment from the Defendant—which Caesars paid.

42. Plaintiff and Class Members have already incurred or will incur out of pocket costs as a result of the Data Breach.

43. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and other accounts for fraud, researching and disputing suspicious or fraudulent activity, obtaining and reviewing credit reports, placing credit freezes on their credit profiles, dealing with spam and phishing emails, text messages, and phone calls, and reviewing their financial affairs more closely than they otherwise would have, among other things. These efforts are burdensome and time-consuming and would not have been necessary but for Caesars' data security shortfalls.

[23] *See* Caesars Entertainment, Inc.U.S. Privacy Policy: How We May Use Your Information, https://www.caesars.com/corporate/privacy (last accessed Sept. 28, 2023).

[24] Id.

44. Even in instances where a Class Member is reimbursed for a financial loss due to fraud, that does not make the individual whole again because there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to fraud and identity theft.[25]

1. Loss of Value of PII

45. Plaintiff and Class Members have also suffered a "loss of value of PII."

46. A robust market exists for stolen PII, which is sold and distributed on the dark web and through illicit criminal networks at specific, identifiable prices. Cybercriminals routinely market stolen PII online, making the information widely available to criminals across the world.

47. For example, stolen driver's license numbers can be sold for between $10 and $35 each.[26]

48. Stolen PII is a valuable commodity to identity thieves. The purpose of stealing large blocks of PII, is to use it to for illicit purposes or to sell it and profit from other criminals who buy the data and misuse it.

49. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[27] The Information Commissioner's Office in the European Union, when investigating a hotel data breach at Marriott, noted that "[p]ersonal data has a real value so organi[z]ations have a legal duty to ensure its

---

[25] *See Victims of Identity Theft*, U.S. Dept. of Justice, Nov. 13, 2017, *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 27, 2023).

[26] *See* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 27, 2023); https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited Sept. 27, 2023).

[27] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited Sept. 27, 2023).

security."[28]

50. Nevada law, too, acknowledges that personal information has intrinsic monetary value. Specifically, Nev. Rev. Stat. § 597.810 provides for statutory damages of $750 for unauthorized commercial use of a person's name, voice photograph, or likeness by companies conducting business in Nevada.

51. The value of personal information is increasingly evident in our digital economy. Many companies, including Caesars, collect personal information for purposes of data analytics and marketing. Caesars recognizes the value of personal information, collects it to better target customers to increase its profits, and shares it with third parties for similar purposes, discussed above.

52. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[29]

53. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not by a price at which consumers themselves seek to sell it, but rather in the economic benefit consumers derive from being able to use it. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII leads to a diminution in value of the PII.

---

[28] *See Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, ICO News, July 9, 2019, *available at* https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en. (last visited Sept. 27, 2023).

[29] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

2. Benefit of Bargain Damages

54. Plaintiff and Class Members also suffered "benefit of the bargain" damages.

55. Plaintiff overpaid for Caesars' services that should have been – but were not – accompanied by adequate data security. One component of the cost of Class Members' use of Caesars' services was the implicit promise Caesars made to protect Class Members' PII.

56. Part of the price consumers paid to Caesars was intended to be used to provide adequate data security. Caesars did not do so. Thus, consumers did not get what they paid for.

57. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those that do not, and vice versa. Indeed, if consumers did not value data security and privacy, Caesars would have no reason to tout its data security efforts in its Privacy Policy.

58. Had consumers known the truth about Caesars' deficient data security practices, they would not have stayed at Caesars properties or would have paid less than they did for their rooms.

59. Plaintiff and Class Members did not receive the benefit of their bargain because they paid for data security safeguards they expected but did not receive.

60. Plaintiff and Class Members are entitled to monetary compensation for the various types of damages discussed above.

61. They are also entitled to payment for a robust set of identity protection services, including credit monitoring. Such services are reasonable and necessary here. The stolen PII is historical in nature and can be used for identity theft and other types of financial fraud. There is no question that the PII was taken by sophisticated cybercriminals, increasing the risks to Class Members.

62. Although Caesars offered in its public statements to provide credit monitoring to its loyalty program members, it has only agreed to provide that service for 24 months. This is entirely insufficient to protect Plaintiff and Class Members from the consequences of identity theft, which are serious and long-lasting. Experts recommend that data breach victims obtain identity

protection services for many years after a data breach. Additionally, there is a benefit to early detection and monitoring. Annual subscriptions for comprehensive identity protection services that include three-bureau credit monitoring, alerts on credit inquiries and new account openings, fraud resolution services, dark web monitoring, and identity theft insurance range from $219 to $329 per year. [30] Caesars must provide monetary compensation to Class Members to pay for these services for their lifetimes.

F. Plaintiff and Class Members are Entitled to Injunctive Relief

63. Caesars acted on grounds that apply generally to the Class as a whole. Thus, injunctive relief is appropriate on a class-wide basis.

64. Plaintiff and Class Members are entitled to injunctive relief requiring Caesars to, among other things:

(a) Strengthen its technical and administrative information security controls and adequately fund them for several years;

(b) Submit to regular, independent System and Organization Controls 2 ("SOC 2") Type 2 audits of its enterprise data networks and all security-relevant systems, with scoping and assertion statement established by an independent assessor;

(c) Promptly implement all remediation measures recommended by the SOC 2, Type 2 assessor and any other forensic analysis or incident response entities retained to address the Data Breach;

(d) Implement tokenization or column-level encryption of sensitive PII in all databases;

(e) delete all PII from non-production database environments.

65. These measures are necessary to guard against future data breaches at Caesars

[30] *See* Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done By Spammers, Not Foreign State,* The Wall Street Journal (Oct. 17, 2018), *available at* https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869 (last visited Sept. 27, 2023).

involving Class Members' PII that Caesars continues to retain.

G. Plaintiff's Experience

66. Plaintiff David Lackey is a current rewards member with Defendant Caesars. Plaintiff joined Defendant's rewards program over twenty years ago. In 2023 alone, Plaintiff has stayed at a Caesars property on four separate occasions.

67. To obtain a Caesars Rewards membership, Plaintiff was required to provide his PII to Defendant, including his name, full address, date of birth, drivers' license number, and Social Security number.

68. Upon information and belief, Defendant received and maintains the information Plaintiff was required to provide to obtain his Caesars Rewards membership.

69. Plaintiff is very careful with his PII. He stores any documents containing his PII in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

70. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring his credit.

71. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

72. Despite these efforts, Plaintiff noticed that he received increased text phishing attempts from multiples sources in the weeks following the Data Breach.

73. Plaintiff suffered actual injury and damages from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of intangible property that Caesars obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; (d) loss of time; (e) imminent and impending injury arising

from the increased risk of identity theft and fraud; (f) failure to receive the benefit of his bargain; and (g) nominal and statutory damages.

74. Plaintiff has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to his Social Security number.

75. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

76. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

H. Caesars' Privacy Policy

77. Caesars' Privacy Policy on its website touted its data security safeguards. The Privacy Policy made materially false and misleading representations and omissions to Class Members. The version of Caesars' Privacy Policy prior to the Data Breach stated the following, in relevant part:

Caesars Entertainment, Inc.
U.S. Privacy Policy

> Caesars Entertainment, Inc. and its subsidiaries and affiliates . . . value you as a customer and are committed to respecting your data privacy. In the course of providing you with products and services, we may collect certain information from or about you. We are providing this Privacy Policy to explain our practices and policies for collecting, using and sharing information collected from or about you when you visit, access, or use, or provide information to us in connection with, one of our properties, websites or mobile Apps (referred to together as the "Caesars Services"). By visiting, accessing, or using, or providing information to us in connection with, the Caesars Services, you

expressly consent to our collection, storage, use and sharing of your information as described in this Privacy Policy.

* * *

INFORMATION WE MAY COLLECT.

We collect and use information we believe is necessary to administer and promote our business, provide you with the products and services you request, and to provide a safe and healthy environment to our employees and other customers. We may collect and maintain both personal information and non-personal information needed for these purposes. Your personal information and/or non-personal information will be referred as your "information" in this Privacy Policy.

* * *

HOW WE COLLECT YOUR INFORMATION.

Information You Directly Provide to Us. You may provide information directly to us under a wide range of circumstances, such as when you submit information to us through our websites or mobile apps, use any gaming or non-gaming services at one of our properties, sign up to receive email or text messages from us, sign up to access Wi-Fi at a property, park at a property, install or use one of our mobile apps, sign up for Caesars Rewards, log in as a Caesars Rewards member, book a reservation for a property, enter an online promotion, request information from us, scan your ID at check-in kiosk at a property, apply for casino credit or provide feedback in a survey.

Information Automatically Collected Through the Caesars Websites.

(i) Traffic Data. We automatically track and collect general log information when you visit a website, including your: (A) Internet Protocol (IP) address, (B) domain server, (C) operating system, and (D) type of Web browser as well as the pages you visit on the website (collectively "**Traffic Data**"). Traffic Data does not personally identify you, however, if you choose to provide us with personal information, we may store some items of your personal information and use it with the Traffic Data to better personalize your experience on our websites. We use the Traffic Data to report aggregated website activity and to better understand the needs of our users so we can make informed decisions regarding the content and design of our websites. It enables us to do the following:

- estimate our audience size and usage pattern;
- learn what information is of most and least interest;
- speed up your searches; and

- learn of any possible website performance problems.

We, or our service providers, may also use Traffic Data to identify your physical location to confirm that you are in a jurisdiction where you can use our mobile or online gaming services. We may collect Traffic Data through various technologies including, but not limited to, cookies, IP addresses, and transparent GIFs (Graphics Interchange Format, a software technology also known as a pixel tag).

(ii) Data Collected Using Cookies and Other Technologies. We also automatically collect information from you using cookies and other technologies on our websites. Cookies are small text files offered to your computer by servers in order to keep track of your browser as you navigate a website. Cookies may be stored on your hard drive in which case they remain on your hard drive until deleted, or in temporary memory in which case they are deleted when you shut down your browser or turn off your computer. We may use cookies and similar technologies to identify who you are and may use them when you visit a website, click on our ads, or open our emails. Cookies also enable us to remember your user preferences for our websites. Cookies and other technologies may also be used for site maintenance and analysis, performing network communications, authenticating users, serving contextual advertisements, and protecting against fraud and theft. You can block or remove cookies using your Internet browser's settings. If you block or remove cookies, your ability to perform certain transactions, use certain functionality, and access certain content on the Caesars Websites may be affected. To find out more about cookies, including how to see what cookies have been set on your device and how to manage and delete them, visit www.allaboutcookies.org.

* * *

(vi) Information You Post on the Caesars Websites. If you post information on any public areas of our websites, that information may be collected and used by Caesars, other website users, and the public generally. We strongly recommend that you do not post any information on our websites that allows strangers to identify or locate you or that you otherwise do not want to share with the public.

* * *

Information We Automatically Collect Through Our Mobile Apps, including Location Information. If you install or use one of our mobile apps, we may collect and use information regarding your mobile device, including but not limited to technical information about your mobile device, system and application software, and peripherals, that is gathered periodically to facilitate any upgrades, product support and other services to you (if any) related to the mobile apps, and to provide services or technologies to you. In addition, if you install one of our mobile apps and allow your device to share location information with us, we may be able to automatically identify and collect the location of your mobile device, including GPS location, which is the real-time

geographic location of your mobile device. We may use your location information for any of the reasons disclosed in this Privacy Policy, including, for example, to provide you with more relevant content and useful app features, such as wayfinding services at our properties, or to confirm that you are located in a jurisdiction where you can use our mobile gaming services. We may also use this data for statistical or business-related purposes to improve our products, services and properties. If you allow a mobile app to send you push notifications, your location information may be used to send real-time offers for goods and services at our properties that are close to your location. You may adjust your device settings to turn off push notifications at any time. Location information may also be collected and used to tailor your marketing offers to your specific interests. You may choose not to share your location details with us by adjusting or turning off your mobile device's location services settings. Please note that even if you adjust the settings in your mobile device to turn off location sharing (via GPS data), we may be able to collect information about the location of your mobile device if you are located on one of the Caesars properties through your Wi-Fi, Bluetooth, and other device settings. See "Information We Automatically Collect from Mobile Devices on Caesars Properties" below for more information.

Information We Automatically Collect When You Use Our Wi-Fi Services. If you use Wi-Fi services that we make available at one of our properties, we might collect information about your use of our Wi-Fi services, including your IP address, Wi-Fi information (such as SSID), mobile carrier, the websites you visit, the type of device and browser you are using, your device identification number, bandwidth used and session time. See "Information We Automatically Collect from Mobile Devices on Caesars Properties" below for more information regarding the collection of information regarding your physical location if you are located on one of the Caesars Properties.

Information We Automatically Collect from Mobile Devices on Caesars Properties. If you have a mobile device, are located on one of our properties, and have your Wi-Fi or Bluetooth functionality enabled, we may collect information concerning your mobile device, including the type of device, device ID, and the precise physical location of your device within and around the Caesars Properties (including geolocation and beacon-based location), for analytics and non-marketing related purposes, such as enabling us to understand our customers' preferences and use of our properties, including general traffic patterns. With your consent, we might also use your location information for marketing purposes, such as to provide you with real-time offers and personalized promotions. If you do not want information concerning your precise location to be collected on Caesars Properties, you may adjust your mobile device location sharing settings and disable the Wi-Fi and Bluetooth functionality in your mobile device settings.

Other Information We Collect Relating to Your Gaming and Purchase History and Other Interactions with Us. When you use any of our gaming services or

> make a purchase at any of our properties, we may collect transactional information about these activities and store it with your customer account. We may use this information to determine your Caesars Rewards tier level (if you are a Caesars Rewards member) and to make predictions about your preferences, and interests, future spending and gaming activity. When located on one of our properties, you also may be videotaped or photographed in connection with a security incident or for other surveillance purposes.
>
> * * *
>
> **SECURITY**
>
> We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. With regard to information that you transfer to us through one of our websites or mobile apps, please be aware that no data transmission over the Internet or a wireless network can be guaranteed to be 100% secure. As a result, Caesars cannot guarantee or warrant the security of any information you transmit on or through a website or mobile app, and you do so at your own risk.

78. These representations were misleading because, among other things, Caesars did not "maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."

79. The Privacy Policy also contained material omissions because it failed to disclose that Caesars' data security practices had significant shortfalls regarding its data systems that held consumers' PII.

80. Plaintiff and Class Members provided their PII to Caesars with the reasonable expectation and mutual understanding that Caesars would take reasonable steps to secure the PII from theft. Caesars failed to do so, in violation of its Privacy Policy and other legal duties discussed below.

I. Caesars Failed to Comply with Established Cybersecurity Frameworks and Industry Standards.

81. The FTC has promulgated various guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need

for data security should be factored into all business decision-making.[31]

82. In 2016, the FTC updated its publication titled *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[32] The guidelines noted that:

(a) Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it";

(b) Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

(c) Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

(d) Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

(e) Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

83. In another publication, the FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented

[31] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Sept. 27, 2023).

[32] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Sept. 27, 2023).

reasonable security measures.[33]

84. The FTC has brought many enforcement actions against businesses for failing to adequately protect customer data.

85. Importantly for current purposes, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

87. In its 2019 Privacy & Data Security Update, the FTC noted that "[s]ince 2002, the FTC has brought more than 70 cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data."[34]

88. In this case, Caesars was fully aware of its obligation to use reasonable measures to protect consumers' PII, acknowledging as much in its Privacy Policy. Caesars also knew it was a target for hackers. But despite understanding the risks and consequences of inadequate data security, upon information and belief, Caesars failed to comply with FTC data security obligations.

89. Caesars' failure to adopt reasonable safeguards to protect PII constitutes an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Similarly, the National Institute of Standards and Technology (NIST) provides

[33] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Sept. 27, 2023).

[34] *See Privacy & Data Security Update: 2019*, Federal Trade Commission, 2020, *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf (last visited Sept. 27, 2023).

basic network security guidance enumerating steps to take to avoid cybersecurity vulnerabilities.[35] The NIST guidelines provide valuable insights and best practices to protect network systems and customer data.

91. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[36]

92. Further, cyber security experts have promulgated a series of best practices that should be implemented by hotels, including the following:

(a) Installing appropriate malware detection software;

(b) Monitoring and limiting network ports;

(c) Protecting web browsers and email management systems;

(d) Setting up network systems such as firewalls, switches and routers;

(e) Monitoring and protection of physical security systems; and

(f) Training hotel staff regarding critical points.[37]

93. Caesars' failure to protect Plaintiff and Class Members' PII illustrates Caesars' failure to adhere to the spirit and letter of the FTC guidelines, NIST guidance, and industry best practices.

J. Companies like Caesars are a Frequent Target of Cyber Criminals, and Caesars Was on Notice of the Threat

94. The type of PII collected by the accommodation industry, makes it particularly

---

[35] *See Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Sept. 27, 2023).

[36] *Id*. at Table 2 pg. 26-43.

[37] *See How to Work on Hotel Cyber Security*, Open Data Security, July 23, 2019, *available at* https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/ (last visited Sept. 27, 2023).

appealing to cyber criminals.

95. Trustwave's "2018 Global Security Report" listed hospitality as one of the top three industries most vulnerable to payment card breaches.[38] Other estimates project that hotels are the targets of around 20% of all cyberattacks.[39]

96. In its 2018 Data Breach Investigations Report, Verizon noted that 15% of all data breaches occurring in 2017 involved the accommodation and food services industry.[40] The report noted that there were 338 breaches in the accommodation industry in 2017 alone, including at many of the major hotel brands.[41]

97. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott, Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data breach incidents.[42]

98. "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital system…."[43]

99. 'While hospitality companies have fewer transactions than retail organizations – and thus have data on fewer customers to steal – they collect substantially more valuable and varied personal data for each of their guests. . . . This rich personal data is invaluable to cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks . . . . By enabling further attacks, breaching a hotel provides

[38] *See Why Cybersecurity Matters*, Hotel Management, Oct. 17, 2019, *available at* https://www.hotelmanagement.net/tech/why-cybersecurity-matters (last visited Sept. 27, 2023).
[39] *Id.*
[40] *See Verizon 2018 Data Breach Investigations Report*, 11th Ed., at pp. 5, 25, 27, *available at* https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (last visited Sept. 27, 2023).
[41] *Id.*
[42] *See Timeline: The Growing Number of Hotel Data Breaches*, CoStar.com, April 7, 2020, *available at* https://www.costar.com/article/139958097 (last visited Sept. 27, 2023).
[43] *See Why Cybersecurity Matters*, Hotel Management, Oct. 17, 2019, *available at* https://www.hotelmanagement.net/tech/why-cybersecurity-matters (last visited Sept. 27, 2023).

cybercriminals much more value than breaching a company in almost any other industry."[44]

100. The high risk of data breaches in the hotel industry was widely known throughout the field, including to Caesars.

101. Indeed, Caesars identified in its December 31, 2022 Form 10-K that cyberattacks were a significant risk factor that it faced, noting "Compromises of our information systems or unauthorized access to confidential information or our customers' personal information could materially harm our reputation and business."[45]

102. Thus, Caesars was clearly aware of the high risk of data intrusions and the magnitude of the harm that could result from a breach. Despite the known risks, Caesars failed to adopt reasonable safeguards to protect Class Members' PII.

VI. CLASS ACTION ALLEGATIONS

103. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3).

104. Plaintiff seeks certification of the following nationwide class:

> Nationwide Class: All persons residing in the United States whose PII was acquired by cybercriminals in the Caesars Data Breach.

105. The Nationwide Class asserts claims against Caesars for Negligence (Count I), Negligent Misrepresentation (Count II), Breach of Implied Contract (Count III), Unjust Enrichment (Count IV), and violation of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 (Count V).

106. Under the Restatement (Second) of Conflict of Laws §§ 145 and 188, adopted by Nevada courts and applies to the facts here, Nevada substantive law controls the common law tort

---

[44] *See Cybersecurity in Hospitality: An Unsolvable Problem?*, Paladion Networks, *available at* https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem (last visited Sept. 27, 2023).

[45] *See* Caesars Entertainment, Inc. Form 10-K for the year ended Dec. 31, 2022, at pg. 21 *available at* https://investor.caesars.com/static-files/abff6ce9-34b1-4057-9c78-db6bf146c295 (last visited Sept. 28, 2023).

and contract-based claims of Plaintiff, regardless of Plaintiff's state of residency.

107. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, may be applied on a nationwide basis because Caesars' unlawful conduct was centered in Nevada.

108. In addition or in the alternative, Plaintiff also seeks certification of a statewide subclass under Virginia law.

> Virginia Subclass: All residents of Virginia whose PII was acquired by cybercriminals in the Caesars Data Breach.

109. The Subclass asserts state statutory claims for violation of the Virginia's data breach notification law, Va. Code Ann. § 18.2-186.6(B), *et seq.* (Count VI).

110. Excluded from the Nationwide Class and all Subclasses (collectively the "Class") are Defendant's executive officers and directors, the judges to whom this case is assigned, their immediate family members, and court room staff.

111. Plaintiff reserves the right to amend the definitions of the Classes after having an opportunity to conduct discovery.

112. Numerosity: Fed. R. Civ. P. 23(a)(1). Upon information and belief, the Nationwide Class and statewide Subclass are each so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time. The class size can be determined by information available in Caesars' records, which will be a subject of discovery. On information and belief, there are millions of Class Members in the Nationwide Class, and at least thousands of Class Members in the state Subclass.

113. Commonality: Fed. R. Civ. P. 23(a)(2). There are many questions of "law or fact" common to the Class for purposes of Rule 23(a)(2), including but not limited to:

> (a) Whether Caesars' data security systems prior to the Data Breach complied with applicable data security laws, regulations, industry standards, and other relevant requirements;
>
> (b) Whether Caesars owed a duty to Plaintiff and Class Members to safeguard their PII;
>
> (c) Whether Caesars breached its duty to Plaintiff and Class Members to safeguard their PII;
>
> (d) Whether Caesars knew or should have known that its data security systems were

deficient prior to the Data Breach;

(e) Whether Caesars detected the Data Breach in a timely manner;

(f) Whether Caesars had a contractual obligation, based on its Privacy Policy or otherwise, to adopt reasonable data security measures;

(g) Whether Caesars failed to provide timely and adequate notice of the Data Breach to Class Members;

(h) Whether Caesars' conduct constituted violations of state consumer protection statutes and state data security and breach notification statutes;

(i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of the Data Breach; and

(j) Whether Plaintiff and Class Members are entitled to injunctive relief.

114. Typicality: Fed. R. Civ. P. 23(a)(3). Typicality is satisfied because the claims of Plaintiff and all Class Members derive from the same operative facts. Plaintiff and Class Members all had their PII stolen in the Data Breach. Plaintiff and Class Members have the same basic legal claims against Caesars.

115. Adequacy of Representation: Fed R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent counsel who are highly experienced in data breach class actions and other complex litigation. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class. Plaintiff's counsel have the financial and personnel resources to litigate this matter through all phases of pretrial litigation, trial, and any necessary appeals. Neither Plaintiff nor their counsel have any interests that are contrary to, or conflict with, those of the Class.

116. Predominance: Fed. R. Civ. P. 23(b)(3). Caesars has engaged in a common course of conduct toward all Class Members. The common issues identified above arising from Caesars' conduct predominate over any issues affecting only individual Class Members. The common issues hinge upon Caesars' conduct rather than that of any individual Plaintiff or Class member. Adjudication of the common issues in a single action has important and desirable advantages that will lead to judicial economy.

117. Superiority: Fed. R. Civ. P. 23(b)(3). A class action is superior to other available

methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law of fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claims is prohibitively high and they would therefore have no realistic means to a remedy on an individual non-class basis. The litigation of separate actions by consumers would create a risk of inconsistent or varying adjudications, which could establish incompatible standards of conduct for Caesars. In contrast, conducting this action on a class-wide basis presents fewer management difficulties, conserves judicial and party resources, and pursues the rights of all Class Members in a single proceeding.

118. Injunctive Relief: Fed. R. Civ. P. 23(b)(2). Caesars acted on grounds that apply generally to the Class as a whole. Caesars continues to retain Class Members' PII, which is subject to potential future data breaches in Caesars' hands. Injunctive relief is appropriate on a class-wide basis.

VII. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or in the Alternative, Negligence According to the Applicable State Subclass)

119. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

120. As a condition of receiving Caesars' services, Plaintiff and all Class Members were obligated to provide Caesars with their PII.

121. Plaintiff and Class Members entrusted their PII to Caesars with the understanding that Caesars would take reasonable measures to safeguard their PII.

122. Caesars had knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could face if their PII was stolen in a data breach.

123. Caesars had a duty to exercise reasonable care in safeguarding, securing, and protecting Class Members' PII. This duty included, among other things, designing, maintaining,

and testing Caesars' data security procedures to ensure that the PII was adequately protected, that cloud-based safeguards were adequately implemented, and that employees tasked with maintaining PII were adequately trained on cyber security measures.

124. Caesars' duty of care arose from, among other things:

- the special relationship that existed between Caesars and its customers because, *e.g.*, Caesars was in an exclusive position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;
- Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;
- Caesars' representations in its Privacy Policy;
- general common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar circumstances would act; and
- state statutes requiring reasonable data security measures, including but not limited to Nev. Rev. Stat. § 603A.210, which states that businesses possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

125. Caesars was subject to an "independent duty," untethered to any express contract between Caesars and Class Members. Sources of the independent duty are included in the list above.

126. Caesars' violation of the FTC Act and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

127. Plaintiff and Class Members were the foreseeable victims of Caesars' inadequate data security practices. Caesars knew that a breach of its systems could cause harm to Plaintiff and

Class Members.

128. Caesars' conduct created a foreseeable risk of harm to Plaintiff and Class Members. Caesars' misconduct included its failure to adequately restrict access to its cloud server that held consumers' PII.

129. Caesars knew or should have known of the inherent risks in collecting and storing PII, the importance of providing adequate data security, and the frequent cyberattacks aimed at the hotel industry.

130. Plaintiff and Class Members had no ability to protect their PII once it was in Caesars' possession and control. Caesars was in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

131. Caesars, through its actions and inactions, breached its duties owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII while it was in Caesars' possession and control.

132. Caesars inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

133. But for Caesars' breach of duties, consumers' PII would not have been stolen by a computer hacker.

134. There is a temporal and close causal connection between Caesars' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

135. As a result of Caesars' negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of damages alleged herein.

136. Due to Defendant's conduct, Plaintiff and Class Members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken is historical and can be used towards identity theft and other types of financial fraud against the Class Members. There is no question that this PII was taken by sophisticated cybercriminals increasing the risks to the Class Members. The consequences of identity theft are serious and long-lasting. There is a benefit to

early detection and monitoring. Some experts recommend that data breach victims obtain credit monitoring services for many years after a data breach. Annual subscriptions for comprehensive credit monitoring plans that include inquiry alerts, credit locks, and identity theft insurance range from $219 to $329 per year.[46]

137. Plaintiff and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth above.

COUNT II
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

138. Plaintiff re-allege and incorporates by reference all preceding allegations as if fully set forth herein.

139. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which imposes liability for negligent misrepresentations based on omissions. Section 551, titled "Liability for Nondisclosure," states:

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if . . . he is under a duty to the other to exercise reasonable care to disclose the matter in question.

140. Caesars failed to disclose to Plaintiff and Class Members that it did not employ reasonable safeguards to protect consumers' PII.

141. Caesars' omissions were made for the guidance of consumers in their transactions with Caesars'.

142. Caesars failed to disclose facts that Caesars knew may justifiably induce consumers to act or refrain from acting in their business transactions with Caesars.

143. Caesars' omissions were made in the course of Caesars' business.

[46] Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done By Spammers, Not Foreign State.* The Wall Street Journal (Oct. 17, 2018), available at: https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869 (last visited Sept. 27, 2023).

144. Caesars had a duty to speak regarding the inadequacy of its data security practices and its inability to reasonably protect consumers' PII.

145. Caesars knew or should have known that its data security practices were deficient.

146. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its data security practices were insufficient to guard against those attacks.

147. Caesars was in a special relationship with, or relationship of trust and confidence relative to, consumers. Caesars was in an exclusive position to ensure that its safeguards were sufficient to protect against the foreseeable risk that a data breach could occur. Caesars was also in exclusive possession of the knowledge that its data security processes and procedures were inadequate to safeguard consumers' PII.

148. Caesars' omissions were material given the sensitivity of the PII maintained by Caesars and the gravity of the harm that could result from theft of the PII.

149. Data security was an important part of the substance of the transactions between Caesars and consumers.

150. Caesars knew that consumers would enter into business transactions under a mistake as to facts basic to the transactions. Because of the relationship between the parties, consumers would reasonably expect a disclosure of the basic facts regarding Caesars' inadequate data security.

151. Had Caesars disclosed to Plaintiff and Class Members that its systems were not secure and thus were vulnerable to attack, Plaintiff and Class Members would not have entrusted their PII to Caesars.

152. Caesars should have made a proper disclosure to consumers when accepting hotel reservations, during the check-in process, or by any other means reasonably calculated to inform consumers of its inadequate data security.

153. In addition to its omissions, Caesars is also liable for its implied misrepresentations. Caesars required consumers to provide their PII during the reservation and/or check-in process. In

doing so, Caesars made implied or implicit representations that it employed reasonable data security practices to protect consumers' PII. By virtue of accepting Plaintiff's PII during the reservation and check-in process, Caesars implicitly represented that its data security processes were sufficient to reasonably safeguard the PII. This constituted a negligent misrepresentation.

154. Caesars failed to exercise reasonable care or competence in communicating its omissions and misrepresentations.

155. As a direct and proximate result of Caesars' omissions and misrepresentations, Plaintiff and Class Members suffered the various types of damages alleged herein.

156. Plaintiff and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

COUNT III

BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

157. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

158. When Plaintiff and Class Members provided consideration and PII to Caesars in exchange for Caesars' services, they entered into implied contracts with Caesars under which Caesars agreed to adopt reasonable steps to protect their PII.

159. Caesars solicited and invited Plaintiff and Class Members to purchase its services. As part of that process, Plaintiff and Class Members were required to provide their PII.

160. When entering into the implied contracts, Plaintiff and Class Members reasonably believed and expected that Caesars would implement reasonable data security measures and that Caesars' data security practices complied with relevant laws, regulations, and industry standards. Caesars knew or reasonably should have known that Plaintiff and Class Members held this belief and expectation.

161. When entering into the implied contracts, Caesars impliedly promised to adopt reasonable data security measures. Caesars required consumers to provide their PII during the

reservation and/or check-in process. In doing so, Caesars made implied or implicit promises that its data security practices were reasonably sufficient to protect consumers' PII. By virtue of accepting Plaintiff's PII during the reservation and check-in process, Caesars implicitly represented that its data security processes were reasonably sufficient to safeguard the PII.

162. Caesars' conduct in requiring consumers to provide PII as a prerequisite to the use of Caesars' services illustrates Caesars' intent to be bound by an implied promise to adopt reasonable data security measures.

163. Plaintiff and Class Members would not have provided their PII to Caesars in the absence of Caesars' implied promise to keep the PII reasonably secure.

164. Plaintiff and Class Members fully performed their obligations under the implied contracts with Caesars. They provided consideration and their PII to Caesars in exchange for Caesars' services and its implied promise to adopt reasonable data security safeguards.

165. Caesars breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures.

166. As a result of Caesars' conduct, Plaintiff and Class Members have suffered, and continue to suffer, legally cognizable damages arising from the Data Breach as set forth above.

167. Plaintiff and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

168. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

169. This claim is plead in the alternative to the breach of implied contract claim.

170. Plaintiff and Class Members conferred monetary benefits on Caesars.

171. In exchange, Plaintiff and Class Members should have received Caesars' services as well as adequate safeguarding of their PII.

172. Caesars profited from its transactions with Class Members in two ways. First, Caesars received monetary consideration as revenue. Second, Caesars used Class Members' PII for a variety of profit-generating purposes beyond simply providing its services. Caesars used the PII for marketing and other purposes discussed more fully above. Caesars used the PII to generate future stays from consumers and derive future revenues and profit.

173. The money Plaintiff and Class Members paid to Caesars were intended to be used by Caesars, in part, to fund Caesars' costs of providing reasonable data security.

174. Caesars failed to provide reasonable data security, yet it kept all monies paid by Plaintiff and Class Members.

175. GM knew that Plaintiff and Class Members conferred monetary and other benefits on Caesars. Caesars accepted those benefits.

176. Under principles of equity and good conscience, Caesars should not be permitted to retain the full monetary benefit of its transactions with Plaintiff and Class Members. Caesars failed to adequately secure consumers' PII and, therefore, did not provide the full services that consumers paid for.

177. Caesars acquired consumers' money and PII through inequitable means in that it failed to disclose its inadequate data security practices when entering into transactions with consumers and obtaining their PII.

178. If Plaintiff and Class Members would have known that Caesars employed inadequate data security safeguards, they would not have agreed to transact with Caesars or would have transacted only at reduced prices.

179. Class Members have no adequate remedy at law. Caesars continues to retain Class Members' PII while exposing the PII to a risk of future data breaches while in Caesars' possession. Caesars also continues to derive a financial benefit from using Class Members' PII.

180. As a direct and proximate result of Caesars' conduct, Plaintiff and Class Members have suffered the various types of damages alleged herein.

181. Caesars should be compelled to disgorge into a common fund or constructive trust,

for the benefit of Class Members, the proceeds that they unjustly received from Class Members. In the alternative, Caesars should be compelled to refund the amounts that Class Members overpaid for Caesars' services.

COUNT V

VIOLATION OF THE NEVADA CONSUMER FRAUD ACT
Nev. Rev. Stat. § 41.600
(On Behalf of the Nationwide Class)

182. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

183. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states:

> 1. An action may be brought by any person who is a victim of consumer fraud.
>
> 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

184. In turn, Nev. Rev. Stat. § 598.0923(2) (a section of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." Caesars violated this provision because it failed to disclose the material fact that its data security practices were deficient and that its cloud server security settings were not adequate to protect consumers' PII. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the omission. Caesars could and should have made a proper disclosure when accepting hotel reservations, during the check-in process, in the registration for its Caesars Rewards loyalty program, in its Privacy Policy, or by any other means reasonably calculated to inform consumers of its inadequate data security.

185. Also, Nev. Rev. Stat. § 598.0923(3) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." Caesars violated this provision for several reasons, each of which is an independent predicate act for purposes of violating § 598.0923(3).

186. *First*, Caesars breached a Nevada statue requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain *reasonable security measures* to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." (Emphasis added.) Caesars is a data collector as defined under the statute at Nev. Rev. Stat. § 603A.030. Caesars failed to implement and maintain reasonable security measures, evidenced by the fact that hackers accessed its cloud server and stole consumers' PII. Caesars' violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3). Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation.

187. *Second*, Caesars breached other state statues as alleged herein. Caesars also violated Nev. Rev. Stat. § 598.0923(2) as alleged in this Count. Caesars knew or should have known that it violated these statutes. Caesars' violation of each of these statutes serves as a separate predicate act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

188. *Third*, Caesars violated the FTC Act, 15 U.S.C. § 45, as alleged above. Caesars knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance for businesses. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were

insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation. Caesars' violation of the FTC Act serves as a predicate act for violating Nev. Rev. Stat. § 598.0923(3).

189. Caesars engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Class Members.

190. Plaintiff and Class Members were denied a benefit conferred on them by the Nevada legislature.

191. Nev. Rev. Stat. § 41.600(3) states that if the plaintiff prevails, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

192. As a direct and proximate result of the foregoing, Plaintiff and Class Members suffered all forms of damages alleged herein. Plaintiff's harms constitute compensable damages under Nev. Rev. Stat. § 41.600(3).

193. Plaintiff and Class Members are also entitled to all forms of injunctive relief sought herein.

194. Plaintiff and Class Members are also entitled to an award of their attorney's fees and costs.

COUNT VI

VIRGINIA DATA BREACH NOTIFICATION LAW V.A. CODE ANN. § 18.2-186.6(b), *et seq.* (On Behalf of the Virginia Subclass)

195. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

196. Caesars is required to accurately notify Plaintiff and Class Members following discovery or notification of a breach of their data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

197. Caesars is an entity that own or license computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

198. Plaintiff and Class Members' Personal Information (e.g., Social Security numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

199. Because Caesars discovered a breach of their security system (in which unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Caesars had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

200. As a direct and proximate result of Caesars' violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Class Members suffered damages, as described above.

201. Plaintiff and Class Members seek relief under Va. Code Ann. § 18.2-186(K), including but not limited to, actual damages.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated individuals, respectfully request the following relief:

(a) An Order certifying this case as a class action;

(b) An Order appointing Plaintiff as a class representative;

(c) An Order appointing the undersigned counsel as class counsel;

(d) Injunctive relief requiring Caesars to: (i) strengthen its data security systems and procedures; (ii) submit to future annual audits of those systems; and (iv) delete PII that Caesars no longer needs for processing services previously provided to Class Members;

(e) An award of compensatory damages, money for significant and reasonable credit monitoring, statutory damages, treble damages, and punitive damages;

(f) An award of Plaintiff's attorneys' fees and litigation costs; and

(g) Such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury as to all issues so triable.

DATED this 29th day of September, 2023.

Respectfully submitted,

KEMP JONES, LLP

/s/ Don Springmeyer

Don Springmeyer, Esq. (NBN 1021)
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, NV 89169

James J. Pizzirusso (*Pro Hac Vice forthcoming*)
Amanda V. Boltax (*Pro Hac Vice forthcoming*)
HAUSFELD LLP
888 16th Street, NW, Suite 300
Washington, D.C. 20006

Steve N. Nathan (*Pro Hac Vice forthcoming*)
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004

Douglas J. McNamara (*Pro Hac Vice forthcoming*)
Brian E. Johnson (*Pro Hac Vice forthcoming)*
COHEN MILSTEIN SELLERS & TOLL, PLLC
1100 New York Ave, 5th Floor
Washington, DC 20005

Counsel for Plaintiff and the Class